City of Virginia Beach

VBgov.com

DEPARTMENT OF POLICE
OFFICE OF INTERNAL AFFAIRS
OFFICE: (757)-385-4145
FAX: (757) 385-4007

MUNICIPAL CENTER
BUILDING 11
2509 PRINCESS ANNE ROAD
VIRGINIA BEACH, VA 23456-9064

September 18, 2018

Mr. Tom Nash
112 Pine Street S
Richmond, VA 23220

RE: Freedom of Information Act Number: FOI2018-2896

Mr. Nash,

This city does not and has not had contracts with the companies Persistent Surveillance System or Vigilant Solutions. We received a donation of 4 units from the City of Norfolk in April of 2011 via the Hampton Roads Urban Area Security Initiative (UASI) grant. We purchased an additional 3 units in September of 2011. All came from a company called Elsag North America, LLC.

Should you have any questions or need further information, I can be reached at (757) 385-4145.

Sincerely,

Investigator A. J. Sargent

Custodian of Records

cc: File

Freedom of Information request may also be requested by clicking the below link and submitting your request.
http://www.vbgov.com/government/departments/police/profstanddiv/Pages/foia-form.aspx

City of Virginia Beach

VBgov.com

DEPARTMENT OF POLICE
OFFICE OF INTERNAL AFFAIRS
INVOICE FOR SERVICES
OFFICE: (757)-385-4145

MUNICIPAL CENTER
BUILDING 11
2509 PRINCESS ANNE ROAD
VIRGINIA BEACH, VA 23456-9064

September 18, 2018

Mr. Tom Nash
112 Pine Street S
Richmond, VA 23220

RE: FOIA / SDT Invoice for Services Number: 2018-2896

City of Virginia Beach Tax ID #54-0722061 Credit to Account Number:			
Amount	Fund	Budget Unit	Object Code
$17.53	002	09010	415007
Date of Service	Description	Amount	Total
September 18, 2018	Search/Redact/Copy/Scan_ $19.43 @	1 /hour	$ 17.53
		Total Due =	$ 17.53

Make check payable to Treasurer, City of Virginia Beach along with remittance to:

Custodian of Records
City of Virginia Beach Police Department
2509 Princess Anne Road
Virginia Beach, VA 23456

Payments made directly to the Treasurer may not be credited to this account.

(Invoice due upon receipt)

Pursuant to §2.2-3704(I),Future Freedom of Information Act requests may be denied to any requestor which has an unpaid balance that is more than 30 days past due.

Sincerely,

Investigator A. J. Sargent

CC: File & Treasurer

All records responsive to the below requests dated from January 1, 2014 through July 28, 2016.

Information/Documents Requested	Response
1. The full documentation of all contracts or non-disclosure agreements (enacted OR IN EFFECT between the above dates) with the companies "Persistent Surveillance Systems" or "Vigilant Solutions"	Does not exist.
2. Copies of all invoices to or from these companies, and documents sufficient to show any and all disbursement of public funds to either company	Does not exist. The equipment was obtained through a grant awarded to another city.
3. The full documentation of all contracts (enacted OR IN EFFECT between the above dates) with any company other than the two cited above, in which said company provides your department with equipment or services (including software) for 1. license plate scanning or reading or automatic photographing; 2. aerial surveillance, excluding monitoring roadways for speed infractions.	We received a donation of 4 LPR units from the City of Norfolk in April of 2011 via the Hampton Roads Urban Area Security Initiative (UASI) grant. We purchased an additional 3 units in September of 2011. All came from a company called Elsag North America, LLC.
4. Copies of all invoices to or from any company that fits the description in the prior paragraph, and documents sufficient to show any disbursement of public funds to any company that fits this description	Does not exist.
5. All emails between police department email accounts and users on the domains "pss-1.com" or "vigilantsolutions.com". (One example would be brian.schockley@vigilantsolutions.com. Users on the domain would be in the form of XXXXXXXXX@vigilantsolutions.com)	Does not exist.
6. All paper-based communications between your department and Persistent Surveillance Systems, and between your department and Vigilant Solutions. In asking for all paper and electronic correspondence, this request necessarily includes marketing materials and descriptions of product capabilities for any device, software, or access/capability this department has purchased. A circuit court judge in Illinois recently ruled that non-disclosure agreements signed by public bodies do not trump freedom of information laws when it comes to surveillance equipment/capability purchased by police. Citation: http://arstechnica.com/tech-policy/2016/01/chicago-police-must-finally-produce-stingray-records-judge-orders/	Does not exist.
7. Documents sufficient to show all rules or regulations governing the use of products (hardware or software) that do 1. license plate scanning or reading or automatic photographing; 2. aerial surveillance, excluding monitoring roadways for speed infractions.	See attached LPR policy
8. The text of all agreements (whether formal, email, memo, or	Does not exist.

Information/Documents Requested	Response
otherwise) between your department and any other public body or department that allows your department to use or access the capabilities of 1. license plate scanning or reading or automatic photographing; 2. aerial surveillance, excluding monitoring roadways for speed infractions. Documents sufficient to show the month and year your department first entered a program of scanning license plates or accessing a database of scanned plates, if it indeed has such a program (and end date of said program if it has ended).	
9. Documents sufficient to show the total number of license plates scanned in your department's jurisdiction (whether the jurisdiction in this case is precisely or roughly represented) since the department began its plate-scanning program or first purchased access to such a program	See the attached. The system only keeps track of statistics going back 3 months.
10. Documents sufficient to show the month and year your department first entered a program of persistent aerial surveillance, if it indeed has such a program (and end date of said program if it has ended).	N/A Does not exist.
11. Documents sufficient to show the number of plane-hours of aerial surveillance (excluding monitoring roadways for speed infractions) purchased by your department within the dates at the top of this request. For example, one plane flying for four hours is four plane-hours. Two planes flying for four hours is eight plane-hours.	N/A Does not exist.
12. Documents sufficient to show any attempt made by a representative of your department to inform the public about automatic license plate readers or persistent aerial surveillance. This could include but is not limited to records of town hall meetings, quotes from police spokespeople in local media, or text from the department's website.	LPR obtained in 2011, press release does not exist.

START	11/09/2005 00:00
END	12/09/2018 23:59

470

DATE	READS TOTAL	ACCEPTED ALARMS	REJECTED ALARMS
2018/06/15	1764	0	0
2018/07/04	526	0	0
2018/07/05	24	0	0
2018/07/06	297	0	0
2018/07/07	130	0	0
2018/07/08	15	0	0
2018/07/21	349	0	0
2018/07/22	526	0	0
2018/07/24	313	0	0
2018/07/25	583	0	0
2018/07/27	939	0	0
2018/08/07	381	0	0
2018/08/14	543	0	0
2018/08/16	306	0	0
2018/08/18	6	0	0
2018/08/21	1208	0	0
2018/08/23	242	0	0
2018/08/24	486	0	0
2018/08/31	40	0	0
TOTAL	8678	0	0

TOTAL	ACCEPTED ALARMS	REJECTED ALARMS
8678	0	0

ALPR (Automatic License Plate Recognition) (CALEA 41.3.9) It is the policy of the Virginia Beach Police Department that no ALPR shall be used, intentionally or otherwise, in a manner that might compromise the legitimate privacy concerns of private citizens. Page 5 of 15 Original: 12-05-2011 - Effective: 08-11-2015 - Amends: 11-20-2014 - Review: 2017 Definitions Automated License Plate Reader (ALPR) – Computer assisted equipment, either fixed or mobile, used to identify and compare license plate numbers. ALPR vehicle: A police vehicle equipped with a system designed to scan and check license plates for stolen status or security threats and then stores the information. Hit – Alert from the License Plate Reader system that a scanned license plate number may be in the NCIC (National Crime Information Center) and VCIN (Virginia Criminal Information Network) database for a specific reason including, but not limited to, being related to a stolen car, wanted person, domestic violence protective order or terrorist-related activity. A hit can also occur based on a scanned license plate that has been manually entered into the database, based on a broadcast BOL (Be On the Lookout). Hot List: Vehicle extract file obtained from the NCIC for use with License Plate Readers that identifies license plate numbers of interest to law enforcement. Hot List Download: The method by which the hot list data is transferred to the reader vehicle computer. Policy/Guidelines for Use (CALEA 41.3.9 A) An ALPR Program Manager shall be designated by the Deputy Chief of Operations. The Program Manager shall be responsible for establishing protocols for: • System Access • Training of Personnel • Data Collection • Data Storage • Data Retention • Conducting monthly and annual audits detailing hits from ALPR and types of clearances for these cases. Monthly audits should be detailed during COMPSTAT meetings while the annual audit shall be included in annual operations division goals and objectives report outs. ALPR systems operated by the Virginia Beach Police Department shall be deployed for law enforcement or Homeland Security purposes only, to include, but not limited to: locating stolen vehicles, carjacked vehicles, stolen license plates, wanted or missing persons, or vehicles on the Hot List; canvassing of areas surrounding recent crimes or for stolen vehicles or stolen tags that may be connected to crime scenes; collecting license plate numbers in areas where intelligence indicates that criminal activity may occur; and analyzing license plate numbers observed frequently at critical infrastructure sites, national icons, or sensitive or secure areas. 1. Prior to usage, the operator of the ALPR shall check the equipment for functionality and camera calibration. Page 6 of 15 Original: 12-05-2011 - Effective: 08-11-2015 - Amends: 11-20-2014 - Review: 2017 2. When in operation, the ALPR scans license plate images without operator action, thus allowing the operator to perform routine patrol operations. 3. The operator receives an audible alert tone and an image of the license plate if a license plate matches one from the current Hot List. The operator must verify that the "captured" license plate matches the wanted license plate. A hit confirmation must be conducted through the Communications Dispatcher. 4. In the event an alert is received on an occupied vehicle, the member must notify Communications and receive confirmation of wanted information prior to initiating a traffic stop. In all instances the member will proceed according to established policy. 5. Any hits on persons listed as "violent gang members" or persons listed on the "terrorist watch list" will provide information to the officers on their status but does not constitute reasonable suspicion to stop a vehicle. This information should be treated like any other intelligence information provided to the officer. If the data collected is determined to be valuable to another law enforcement agency the data may be shared but must clearly be for law enforcement purposes only. The ALPR Program Manager or designee shall be responsible for determining the type of data and best method for disseminating the data to another law enforcement agency. Any data

disseminated shall be documented in a log kept in the ALPR network drive. 6. Any significant incident or arrest utilizing an ALPR shall be documented electronically by the operator prior to the end of shift and forwarded to the operator's supervisor and Departmental ALPR Program Manager. This can be done via e-mail notification. 7. ALPR operators may search past images to determine if a particular license plate was photographed. This feature may be utilized at the request of members or other law enforcement officers for investigative purposes. 8. When not in use, all ALPR equipment will remain in the assigned vehicle. The ALPR trained officer is required to log in to the ALPR system at the beginning of their shift and log out of the ALPR system at the conclusion of their shift. 9. Special requests for ALPR equipped vehicles for planned patrol operations shall be made to the lieutenant or captain approving the patrol plan. The use of an ALPR and any information resulting from the ALPR use shall be documented in the After Action Report and forwarded to the ALPR Program Manager. This information shall be entered into the designated ALPR network folder. 10. ALPR systems are fixed and shall not be altered or adjusted without supervisory approval. 11. System maintenance, repairs, and cleaning shall comply with manufacturer's specifications and will only be accomplished by designated personnel. Page 7 of 15 Original: 12-05-2011 - Effective: 08-11-2015 - Amends: 11-20-2014 - Review: 2017 12. Each command that utilizes and ALPR system shall be responsible for documented quarterly inspections of these systems. Data Security and Access (CALEA 41.3.9 B) Commands shall ensure that the ALPR cars are assigned on all shifts and that the equipment is being used properly. All ALPR units shall be used in accordance with department training and the manufacturer's guidelines and instructions and shall be used for criminal justice/official business only in accordance with the Code of Virginia. Only certified ALPR operators, administrators and designated COMIT Service Administrators shall have access to and operate the ALPR system. ALPR operators will conduct all operations using vendor-supplied software on the assigned vehicle's mobile computer interfacing with the ALPR's processing unit. All software and hardware used with the ALPR shall be approved by ComIT or their designee. Misuse of ALPR may subject the operator, his or her supervisor and/or the agency to criminal, civil and/or administrative sanctions under VCIN/NCIC guidelines. Hot List and Hot List download A. Hot list updates shall only be performed by approved personnel. The Hot List file will be downloaded from the secure Virginia State Police controlled website to the designated network server. The updated Hot List file will automatically be pushed across the secure city network to the mobile computer(s) in the ALPR equipped vehicle(s). The trained ALPR user should confirm that the ALPR system is running the most current Hot List through the Car Systems Application Operations Menu. B. The "hot list" download on the designated network server is to remain protected and confidential as is any information received from the NCIC and VCIN files. Any transfer of data to another shall be considered "secondary dissemination", which is not permitted with the ALPR reader system. Training (CALEA 41.3.9 C) The ALPR Program Manager shall be responsible for proper selection of personnel to attend ALPR training. Training in the operation of any ALPR will be conducted according to the specific ALPR manufacturer guidelines. All training must be documented and on file with Professional Development and Training. Upon completion of training each new operator will be provided and username and password for the ALPR System. Professional Development and Training will maintain a list of qualified ALPR operators. All operating members must have VCIN B Level certification. Page 8 of 15 Original: 12-05-2011 - Effective: 08-11-2015 - Amends: 11-20-2014 - Review: 2017 Data Storage and Retention (CALEA 41.3.9 D) The vendor server will upload the data recorded by the ALPR daily from the mobile computer and transfer the data to a designated file server. In addition,

the designated electronic data administrator(s) will download the license plate image files and the NCIC/VCIN information associated with any stolen/wanted vehicle or stolen license plate captured by the ALPR using a designated USB Flash Drive in the event of a network failure. This data will be transferred to the designated storage device(s) and deleted from the USB Flash Drive immediately following the successful transfer of the data files. If the ALPR is used specifically to gather intelligence information, all of the electronic data obtained should be downloaded to the Crim-intel Database, as opposed to the designated file server. Currently, any data collected shall be retained for 24 hours before being purged. If data collected is determined to be linked to a specific crime, the data may be retained for a period longer than 24 hours. The length of time this data will be stored will be determined the Virginia Record's Retention Schedule. Requiring the video file as evidence for court. The recorded DVD will then be vouchered and submitted to Property and Evidence. ALPR material used for court testimony as evidence will be transferred to a DVD and submitted to Property and Evidence until the case is fully adjudicated to its final conclusion. The ALPR Program Manager shall serve as a video file administrator. The manager shall be responsible for maintaining any video files and providing access to these files for authorized personnel. The program manager shall be responsible for copying any required video files in their entirety to DVD for an officer